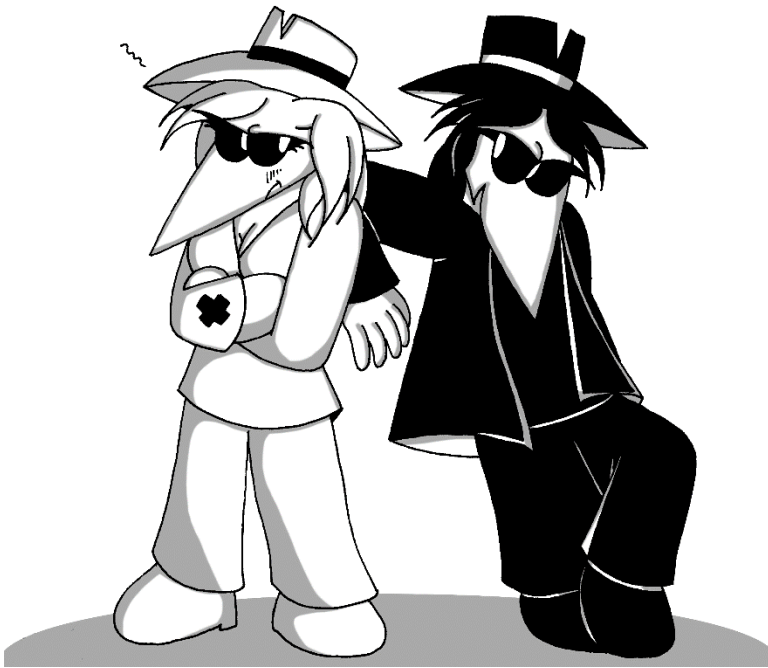


Somebody's Watching You

Government Spying in the Pacific Northwest



Somebody's Watching You

Government Spying in the Pacific Northwest

2nd Edition

August 2024



It's a Trap!

Undercover Cops, Informants, and Cooperating Witnesses

Since 9/11, (actual or perceived) Arabs and Muslims have been viewed by law enforcement as a potential threat on no basis other than religion or ethnic background. Multiple law enforcement agencies – including local police, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) and a partnership of these agencies called the Joint Terrorism Task Force (JTTF) – have diverted public resources to monitoring and entrapping* members of these communities as part of the United States' "War on Terror."

As part of these practices, law enforcement agencies pressure members of the targeted communities to engage in "community policing" to secretly assist in surveillance and entrapment of specific individuals and organizations. Since these tactics by law enforcement are becoming more common, it is important for you to know what types of individuals may be part of community policing. There are three main categories of people who secretly may be collecting information for law enforcement or trying to ensnare you in illegal behavior:

Undercover Cops are police officers who don't identify themselves as such. They may claim to be interested in joining your social/religious/activist group, having political discussions, or worshipping with you.

Informants are not sworn officers employed by the government but they may be paid or coerced or provided other incentives. They are often people with ties to a community or movement or a group who can be leveraged to provide assistance.

Cooperating Witnesses are people who agree to provide information to law enforcement and testify against others usually in exchange for leniency in their own cases.

We will refer to them collectively as "undercover agents." Here are some important things to know → → →

UNDERCOVER AGENTS ARE COMMONLY FROM WITHIN YOUR RELIGIOUS, POLITICAL, CULTURAL, OR ETHNIC COMMUNITIES.

UNDERCOVERS DO NOT HAVE TO TELL YOU THAT THEY ARE WORKING FOR THE POLICE (even if you ask them).

UNDERCOVER AGENTS CAN PARTICIPATE IN, AND EVEN ENCOURAGE, ILLEGAL ACTIVITIES in furtherance of a legitimate law enforcement purpose. For example, they can provide drugs or other contraband to their targets, and they can provide the means or materials to commit a crime.

Somebody's Watching You



Why should we care about our digital footprints, about monitoring and surveillance of our daily activities? Do normal, honest, hard-working people really have anything to hide?

During his 2013 interview of Edward Snowden, in Hong Kong, Glenn Greenwald asked: "Why should people care about surveillance?" Edward Snowden's reply is even more pertinent today than it was in 2013: *"Because even if you're not doing anything wrong, you're being watched and recorded. And the storage capability of these systems increases every year consistently, by orders of magnitude, to where it's getting to the point you don't have to have done*

anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer." (Democracy Now, 2013)

The American Civil Liberties Union (ACLU) stated *"Privacy today faces growing threats from a growing surveillance apparatus that is often justified in the name of national security. Numerous government agencies—including the National Security Agency, the Federal Bureau of Investigation, the Department of Homeland Security, and state and local law enforcement agencies—intrude upon the private communications of innocent citizens, amass vast databases of who we call and when, and catalog "suspicious activities" based on the vaguest standards. The government's collection of this sensitive information is itself an invasion of privacy. But its use of this data is also rife with abuse. Innocuous data is fed into bloated watchlists, with severe consequences—innocent individuals have found themselves unable to board planes, barred from certain types of jobs, shut out of their bank accounts, and repeatedly questioned by authorities. Once information is in the government's hands, it can be shared widely and retained for years, and the rules about access and use can be changed entirely in secret without the public ever knowing."* (ACLU, 2022)

Even the most truthful and innocent comment can be used to bring criminal charges against you, or to get you listed as a “threat” by some government agency. U.S. Supreme Court Justice Stephen Breyer, writing in *Rubin v. United States* 524 U.S. 1301 (1998) stated: *“The complexity of modern federal criminal law, codified in several thousand sections of the United States Code and the virtually infinite variety of factual circumstances that might trigger an investigation into a possible violation of the law, make it difficult for anyone to know, in advance, just when a particular set of statements might later appear (to a prosecutor) to be relevant to some such investigation.”*

It may be true that you have nothing to hide, but it is also true that most people have things about their lives that they consider private, things that they don’t share with the public at large and things that should not be monitored and recorded by government agencies *“based on the vaguest standards”*.

Even if government agencies are not monitoring and surveilling you for official purposes, police and government agents are misusing confidential government databases to stalk and harass innocent victims, and retaliate against whistleblowers and others who speak out against government misconduct.

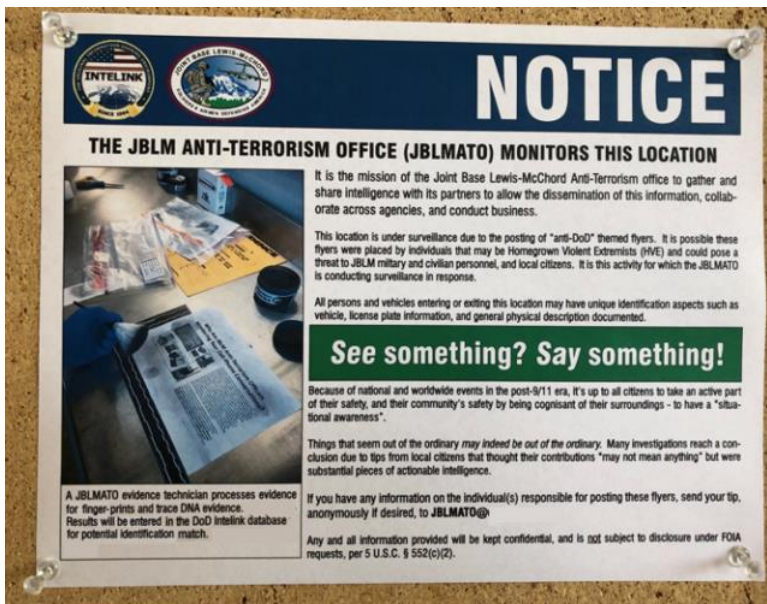
“Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business

associates, neighbors, journalists and others for reasons that have nothing to do with daily police work, an Associated Press investigation has found. Criminal-history and driver databases give officers critical information about people they encounter on the job. But the AP's review shows how those systems also can be exploited by officers who, motivated by romantic quarrels, personal conflicts or voyeuristic curiosity, sidestep policies and sometimes the law by snooping. In the most egregious cases, officers have used information to stalk or harass, or have tampered with or sold records they obtained.” (Gurman, 2016)

The Center for Constitutional Rights stated *“unconstitutional government spying and infiltration have regularly been used to disrupt and entrap social movements, activists, and members of vulnerable communities. In the post-9/11 era, surveillance has undermined and fundamentally reoriented our democratic institutions: mass collection of data on ordinary citizens is no longer the exception, but the rule.”* (Center for Constitutional Rights, 2022)

In 2019, the Joint Base Lewis-McChord [WA] Anti-Terrorism Office (JBLMATO) posted notices in the civilian communities around the military base and conducted surveillance of off-base businesses after community members protested the use of Stingray electronic surveillance devices to monitor their cellular telephone communications. After members of the civilian community posted warnings about the use of

Stingray, the JBLMATO responded with its own notice, warning that the businesses that objected to the surveillance of the civilian community by the military were being placed under surveillance, and calling the individuals who posted warnings of the illegal military surveillance, “Homegrown Violent Extremists” because they had dared question the government and had posted “anti-DOD themed flyers”.



Joint Base Lewis-McChord (JBLM) later claimed that the JBLMATO Notices posted in the civilian community were not an “official” activity of the military base. It should be noted however that the JBLMATO has a long history of surveillance and monitoring of the civilian community when community

members engaged in political protests and advocacy in opposition to government policy.

Why Are JBLM Anti-Terrorism Officers Monitoring Your Cell-Phone Conversations?



- In November 2018, the Tacoma News Tribune reported that, "Tacoma has appealed a court decision that resulted in a nearly \$300,000 payout after a judge ruled the city violated state law by withholding records related to a police surveillance device called a cell site simulator. In paperwork filed last week, Tacoma asked the Washington State Court of Appeals to review the ruling by Pierce County Superior Court Judge Helen G. Whitener. The judge found the city violated the state Public Records Act by deliberately withholding 11 records from the American Civil Liberties Union and three Tacoma plaintiffs. The documents concerned the use of the surveillance device — known as a Stingray — which mimics a cell phone tower and compels all nearby devices — not just the target's phone — to connect to it. That concerned the ACLU and other civil liberties or privacy-focused groups. For violating the records law Whitener said June 25, Tacoma should pay \$182,340, plus \$115,530 for attorney fees and other costs."
- In a January 2019 motion for a protection order to prohibit the release of information to the public and the press, Joint Base Lewis-McChord (JBLM) expressed a concern about public disclosure of information alleging that Anti-Terrorism Officers in the JBLM Directorate of Emergency Services (DES) "were using Stingray, electronic warfare equipment, to unlawfully spy on citizens." (Why would JBLM seek to conceal this if it wasn't true?)



Federal law enforcement agencies have a dark history of targeting political and progressive movements. Some of the dirty tricks they use against these movements include: infiltration of organizations to discredit and disrupt their operations; campaigns of misinformation and false stories in the media; forgery of correspondence; fabrication of evidence; and the use of grand jury subpoenas to intimidate activists.

Today American citizens must know and understand the threat posed by federal law enforcement agents and their tactics as well as several key security practices that offer the best protection against their illegal tactics.

See: (Panagacos v. Towery, 782 F.Supp. 2d 1183 (2011))

And just what "anti-DOD themed flyers" were being posted in the community, that caused the JBLMATO to declare that those posting those fliers were "Homegrown Violent Extremists"? Apparently, the fliers did nothing more than ask 'Why Are JBLM

Anti-Terrorism Officers Monitoring Your Cell-Phone Conversations?” and warned the community about their illegal surveillance tactics.

In her book, Spying on Democracy, Heidi Boghosian, the former director of the National Lawyers' Guild, wrote about the JBLMATO saying: *“In the words of the government agencies involved, they aimed to neutralize PMR [Port Militarization Resistance, a political group that opposed the war in Iraq] through a **pattern of false arrests and detentions, attacks on homes and friendships, and attempting to impede members from peacefully assembling and demonstrating anywhere, at any time. Harassment was systematic and pervasive...** The case revealed that today's military has continued to engage in COINTELPRO-type operations and shows the extent to which the lines between the military and civilian law enforcement have blurred. Forces now used against ordinary people engaged in free speech and protest include, increasingly, weapons and tactics used by the U.S. military for combat missions. The drift from passive intelligence gathering to offensive counterintelligence is one manifestation of the difference between civilian law enforcement principles and the military's exclusive focus on defeating perceived enemies through combat, propaganda, and covert operations... The role of civilian law enforcement, in theory, is to protect the public and the Constitution whereas the role of the military is to identify the enemy and neutralize them... When the*

military starts identifying peaceful dissenters here as the enemy, God help us all."

According to an article in the Northwest Guardian, the official newspaper of Joint Base Lewis-McChord, Army antiterrorism officers on the military base asked both the military and civilian communities to report questionable social media posts to them.



There's no such thing as too vigilant, official says

Laura M. Levering/Northwest Guardian

Dan Vessels, antiterrorism officer, said nothing is too trivial to report. People observing the installation, taking photographs, soliciting questions, questionable postings on Twitter or Facebook or anything that seems out of place should be reported to officials.

"If you see something that doesn't seem right, report it and let the right people determine if it's right or wrong," Vessels said.

The community can report suspicious activity to the JBLM Protection Division Facebook page or Twitter account. Both are monitored 24/7. They can also call the office at 966-7319/7317.

"Nothing is too trivial to report... questionable postings on Twitter or Facebook or anything that seems out of place should be reported to officials."

And, according to the article, the antiterrorism office states that "nothing is too trivial to report". This type of monitoring has a chilling effect on the 1st Amendment rights of American citizens when even the most trivial comment on social media is being collected and databased government agents. (Levering, 2011)

It appears that the JBLMATO even set up their own Facebook and Twitter accounts to encourage reporting of activities in the civilian community and to

move the reporting method outside of official military channels where it might be identified as being unauthorized, or become the subject of a request under the Freedom of Information Act (FOIA).

It is clear that collecting information about individuals because of their social media posts, violates Federal law and regulations. In accordance with DoD Directive 5240.01 and E.O. 12333, it is DoD policy that: [DoD Personnel] *“May not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States”* but that doesn’t mean that some corrupt government agent isn’t collecting information about even your most trivial social media posts and comments.

The image displays two screenshots of official military communications. The left screenshot, dated 3 January 2022, is titled 'JBLM suspicious activity reporting tools' and lists contact information for the Joint Base Lewis-McChord Police and other agencies. It also features logos for 'REPORT SUSPICIOUS ACTIVITY' and 'Eagle Eyes WATCH, REPORT, PROTECT'. The right screenshot, dated 6 JAN 2022, is titled 'JBLM Area Events' and lists various events, including 'NATIONWIDE VIGIL FOR DEMOCRACY' and 'March For Freedom'. A red circle highlights the 'March For Freedom' event details. Both screenshots include logos for the Department of Defense and the Joint Base Lewis-McChord.

In January 2022, the San Francisco Bay Area Independent Media Center (Indybay), reported that the ‘JBLM DES Protection Division [is] Still Illegally Spying on You’, revealing that the JBLM DES

Protection Division was collecting and disseminating information about a "Vigil for Democracy" and a "March for Freedom"? Both of these events were peaceful political rallies that had no connection to JBLM or the military in general. This type of government monitoring has a chilling effect on 1st Amendment protected speech and political activities. (JBLM Cop Watch, 2022)

Emails show that, from 2016 to 2023, the Medford [Oregon] Police Department coordinated heavy-handed police responses to peaceful rallies and protests, tracked activist groups' social media pages, and consistently treated typical, First Amendment-protected activity as a potential crime worthy of law enforcement scrutiny... **the emails show a policing apparatus that treats even the most placid social justice activities — like vigils and Juneteenth celebrations — as sites of criminal threat.** (Lennard, 2023)

According to the ACLU of Washington - For years, with seemingly little to no oversight, the Naval Criminal Investigative Service (NCIS) has been monitoring vast amounts of non-military U.S. Internet traffic and communications, looking for evidence of criminal activity. A NCIS officer, monitoring computers in the state of Washington, believed he was entitled to conduct Internet surveillance of any computer within a specific jurisdiction and did not have to limit his monitoring to U.S. military or government computers or personnel. The problem? The individuals being

monitored by NCIS, like most residents of Washington, are civilians and had no connection to the military. The Posse Comitatus Act (PCA), a federal statute enacted in 1876, prohibits the military from investigating civilians and otherwise participating in civilian law enforcement activities.

The ACLU goes on to state *"The PCA's legal protections are crucial to preserving the important constitutional limitations on military involvement in civilian activities. While the military should know these limits, as we've uncovered through Freedom of Information Act requests, it has repeatedly conducted improper civilian surveillance. That includes U.S. Army-issued National Security Letters, a honey pot established by the Air Force that violated the Foreign Intelligence Surveillance Act and an order of the Foreign Intelligence Surveillance Court, and Army Cyber Counterintelligence officers covertly attending the Black Hat computer security conference without proper authorization.*

While the PCA is a criminal statute, it appears the government has never charged anyone with violating it since it passed 136 years ago. Given the history of improper military excursions into civilian affairs, the expansive Internet surveillance that occurred here, and the fact technological advancements make it easier for the military to conduct widespread Internet surveillance, the only way to deter military officials from intruding into

civilian affairs is to exclude evidence it improperly obtains." (Fakhoury, 2015)

In August 2021 the FBI arrested a Washington State man after the man's mother posted a photo on Facebook of the man participating in the January 6th Capitol Riot in Washington DC. "According to a criminal complaint, two of [the man's] relatives saw on Facebook what appeared to be a photo of him inside of the Capitol Building on Jan. 6, 2021. The two family members reported the image and were interviewed by police." Police then reviewed the mother's Facebook and arrested the man in question. (Q13 Fox News, 2021)

In a 2018 probable cause statement, written as part of a District Court Violation Notice (DCVN) – (a DCVN may be issued by a federal law enforcement officer for violations of certain federal laws and, if occurring on federal property, certain state laws. Violations include improper parking, illegal camping, speeding, civil disturbances, fish and wildlife infractions, and other offenses) JBLM DES Military Police Investigators (MPI) stated that they had "conducted a link analysis from open-source collection of **everything published, by the subject of the MPI investigation, accessible on the Internet.**" This type of broad collection of information about a person - even through open source - is specifically prohibited by DOD regulations, but this prohibition was, it seems, simply ignored by the JBLM MPI. – It is, however, just this type of broad, sweeping

collection that Edward Snowden warned about in 2013, when he said *“it’s getting to the point you don’t have to have done anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use the system to go back in time and scrutinize every decision you’ve ever made, every friend you’ve ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer”*.

Everything that we do, on-line, via cellular networks, in e-mail, on social media, or anywhere in cyberspace has the potential to be monitored, recorded, and used to harm us in some way. This monitoring and surveillance is massive government over-reach and abuse of authority, showing a complete disregard to the privacy rights and civil liberties of those people caught in their intrusive dragnets. Therefore, we must take steps to protect ourselves in cyberspace, just as we do in the physical world.

A search of your electronic life is not your only concern. Government agents can infiltrate private, political, and activist organizations. We saw an example of this illegal infiltration of these organizations in the case of *Panagacos v. Towery*, 782 F.Supp.2d 1183, 1191 (W.D. Wash. 2011) where personnel from the Joint Base Lewis-McChord DES Protection Division’s Anti-Terrorism Office

(JBLMATO), in Washington state, infiltrated political organizations opposed to the war in Iraq.

According to an article in the Olympian Newspaper, Ex-worker at JBLM Collected Activist Data *“A former Joint Base Lewis-McChord employee who spied on war protests in Olympia helped compile detailed information on protesters, including their names, photos, addresses and, in some cases, Social Security numbers, according to 133 pages of law enforcement records released by the City of Tacoma.” The documents detail years of surveillance of protest groups by Joint Base Lewis-McChord and the South Sound Regional Intelligence Group. The detailed information collected about the protesters continues to be stored by area law enforcement agencies to this very day.”* (Pawloski, 2011)

It should be noted that DOD regulations prohibit this type of collection, stating *“No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information... without specific prior approval by the Secretary of Defense, or his designee.”* (DoDD 5200.27)

An article in Defending Rights and Dissent, reported that "New Records Reveal Army Infiltrator Orchestrated Multi-Agency Spy Ring Targeting Leftists, Anarchists Army illegally supplied intelligence on nonviolent antiwar protesters to FBI and police in multiple states." An informant was paid by the Army to infiltrate political groups and share unlawfully obtained

intelligence with a growing network of law enforcement agencies, including the FBI, and police departments in Los Angeles, Portland, Eugene, Everett, and Spokane. The informant (Towery) who worked at Joint Base Lewis-McChord, not only coordinated his actions with local, state and federal law enforcement agencies, many of whom are named defendants in the *Panagacos v. Towery* case, he also admitted to eavesdropping on a confidential, privileged attorney-client email listserv of criminal defendants and their legal counsel. Such conduct is a constitutional violation, but Towery also took sensitive information from the listserv vital to a pending criminal trial and passed it on to Washington State Fusion Center officials who then transmitted it to prosecutors, forcing a mistrial in a case the defense was winning handily. The case was later dismissed for prosecutorial misconduct. (*Defending Rights and Dissent*, 2014)

Pierce County Sheriff's Det. Chris Adamson, director of the Washington State Fusion Center's "Intelligence Group 5" and one of Towery's [handlers] said in a March 26, 2014 deposition that he used intelligence from Towery to place activists on a widely disseminated domestic terrorism list used by law enforcement. Adamson had no trouble equating sit-ins and civil disobedience blockades with domestic terrorism "if they were trying to obstruct governmental process" or if "they're tying up law enforcement resources."

Both Towery and his supervisor at Joint Base Lewis-McChord - DES Protection Division Chief Thomas R. Rudd - admitted to anonymously spying on email listservs run by various political groups. Towery, Rudd and other Army personnel also violated Posse Comitatus, which prohibits the military from enforcing domestic laws on U.S. soil. [Note: Thomas Rudd retired from JBLM in 2019, and was replaced as Chief of the JBLM DES Protection Division by Daniel L. Vessels.]

Towery's information was circulated to police departments in multiple states, and used to disrupt planned protests by **preemptively and falsely arresting activists**.

"On multiple occasions, PMR activists were pulled over on their way to protests and arrested on bogus charges that were later dismissed. Activists engaged in symbolic civil disobedience were violently attacked by police and arrested en masse. Information obtained surreptitiously by the Army was used to disrupt a criminal prosecution then under way in state court. The Army even distributed dossiers on some of the plaintiffs to law enforcement, characterizing the activists as terrorist threats." (Hermes, 2017)

After an Army investigation in 2009, Thomas Rudd said he was reprimanded for his conduct but, despite this, Rudd admitted in an April 2014 deposition that he continued to anonymously spy on email listservs and social media postings of political

activists throughout Washington, Oregon, and California.

The JBLM DES Protection Division / JBLMATO engaged in a multi-year pattern of illegal spying on political activists, monitored electronic communications, created databases containing the personal identifying information of American citizens, and labeled them domestic terrorists for peacefully protesting government policy. Even after being ordered to stop their illegal activity, according to court depositions, government employees in the Protection Division continued to anonymously spy on American citizens and monitor their communications. This illegal collection of information about, and surveillance of, American citizens by government civilian employees in the JBLM DES Protection Division / JBLMATO continues even to this very day.

Government bullying and retaliation by JBLM against anyone reporting illegal activities of the Protection Division / JBLMATO is of great concern. Of perhaps even greater concern is the use of false information, manufactured evidence, and perjured testimony in reports by JBLM law enforcement. Because of the JBLMATO's official misconduct and false reporting; JBLM Military Police Investigations (MPI) law enforcement reports have been tainted with false information, and individuals who have committed no crime have been charged with offenses that they did not commit. The corruption of the JBLM DES has spread like a plague, infecting other JBLM agencies

as well as off-post agencies that have received JBLM DES false and malicious reporting and entered information from JBLM into their own records and systems of records.

If you question JBLM's illegal activities, or request information about the military base through the Freedom of Information Act (FOIA) you are very likely to become a target of on-going surveillance and monitoring by the JBLM DES Protection Division.

SWORN STATEMENT			
For use of this form, see AR 190-45; the proponent agency is PMG.			
PRIVACY ACT STATEMENT			
AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).			
PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.			
ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.			
DISCLOSURE: Disclosure of your SSN and other information is voluntary.			
1. LOCATION	2. DATE (YYYYMMDD)	3. TIME	4. FILE NUMBER
Joint Base Lewis McChord, WA	20171031	1300	
5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS	
Vessels, Dan		GS-12	
8. ORGANIZATION OR ADDRESS			
Directorate of Emergency Services (DES), JBLM Garrison			
9. I, <u>Dan Vessels</u> , WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:			
Q8. There have been various ICE comments submitted by someone who claims to be an MP. Did you have any of the below conversations with an MP? If so, what was your recollection of the conversation?			
e. Keeping track of a guy named Drew Hendricks			
Answer: Yes, Drew Hendricks is our #1 anarchist protestor. He organizes protests and does FOIA requests on us. I have had the discussion with people in the line of duty about Drew Hendricks and how we keep an eye on him.			
AFFIDAVIT			
I, <u>Dan Vessels</u> , HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1, AND ENDS ON PAGE <u>3</u> . I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.			
VESSELS, DANIEL LEE. 1104859794			
(Signature of Person Making Statement)			

(October 2017 excerpt from a Sworn Statement wherein Mr. Vessels admits to monitoring a local political activist – Drew Hendricks - because he submits FOIA requests. – Obtained via Public Records Request.)

The above excerpt from a sworn statement by JBLM DES Protection Division Chief Daniel L. Vessels confirms that JBLM is monitoring a local

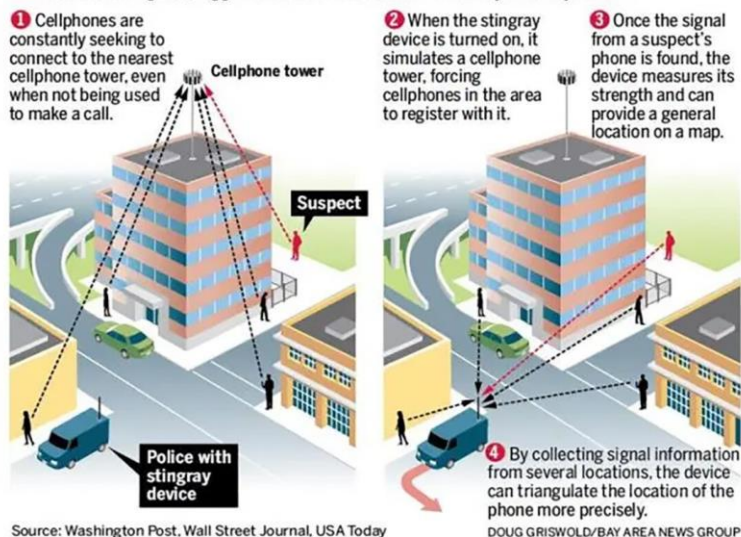
activist, Drew Hendricks because Mr. Hendricks organizes protests and submits FOIA requests for information from JBLM.

Mr. Hendricks was active in the Port Militarization Resistance movement and in peaceful protests against US involvement in the war in Iraq. As a result of his political activities, Mr. Hendricks, like so many others, has been targeted, surveilled, and harassed by JBLM anti-terrorism officers, for years.

Still another example of government agencies abusing their authority was seen in a 2019 motion to the United States District Court for the Western District of Washington, where the Joint Base Lewis-McChord (JBLM) Staff Judge Advocate sought to prevent the defendant in a misdemeanor case from having direct access to the evidence against him, because the government feared that information would be released to the media. Just what information was the government concerned about being released to the media? In the government's own words in the motion: *"It is alleged that [Defendant] has a long-standing professional and personal feud against D.V. and T.R. Several of their arguments stem from [Defendant's] claim that D.V. and T.R. are unlawfully releasing personal identifiable information and collecting intelligence on U.S. citizens. Further, [Defendant]... alleges that JBLM DES is using Stingray, electronic warfare equipment, to unlawfully spy on citizens."*

Secretively tracking cellphones

Law enforcement agencies are using high-tech information-gathering devices to track cellphones. The government considers information about these devices to be sensitive, and not much is known publicly about how the devices are used. Though generally called stingrays, model names for these devices include KingFish, Triggerfish and Hailstorm. Here is basically how they work:



Yes, the government submitted a motion to the court to prevent a defendant in a misdemeanor case from having copies of the evidence against him, in order to conceal the fact that the JBLM military base was conducting illegal surveillance of the civilian community and using Stingray, electronic warfare equipment, to unlawfully spy on citizens.” (Although JBLM was successful in obtaining a court order to seal records showing illegal surveillance of the civilian community, the motion for the protective order acknowledging JBLM's use of 'Stingray electronic warfare devices' is available on Public Access to Court Electronic Records (PACER)).

The use of “*Stingray, electronic warfare equipment, to unlawfully spy on citizens*” was not limited to the JBLM military base, but was also being used by the police department in Tacoma, WA (the city adjacent to JBLM). According to the Tacoma News Tribune newspaper, Tacoma police were “using surveillance devices to sweep up cellphone data” for years. (Martin, 2016)

Like the JBLM military base, the Tacoma Police Department sought to conceal their use of Stingray devices. According to the ACLU of Washington, in 2021, the City of Tacoma was ordered to pay a total of \$311,607 to resolve a case in which the Tacoma Police Department improperly withheld information related to its use of a cell site simulator, an invasive surveillance device.

KOMO 4 News reported that you may be connecting with a device that can trick your phone into thinking it's a cell tower, so it can spy on you. A cell site simulator or Stingray can intercept your phone signal, and essentially trick it into connecting to it and 'potentially suck up all your data' like conversations and text messages. (Esteban, 2018)

Government agencies frequently engage in surveillance of individuals and groups that they deem to be a "threat". That “threat” need not be real, nor it seems, does the government needs probable cause to believe that you have broken the law before targeting you with their surveillance apparatus. And it is not just mass surveillance as we saw in Edward

Snowden's disclosures in 2013. Local police departments or out-of-control personnel from your local military base may be collecting and disseminating information about you, even without any evidence to suggest that you have broken any law.

Brendan Maslauskas Dunn, one of the PMR political activists, wrote: *"Many of us were routinely harassed. My house in Olympia, where I lived with several other activists, was under almost constant surveillance by police. They regularly parked their cars across the street, facing our house, and often came onto our property to harass us. I also discovered that the police at the college I attended kept a picture of me on their wall alongside that of another PMR activist for reasons I am still unaware of. In Tacoma, a surveillance camera was secretly installed on a utility pole across the street from Pitch Pipe. In September 2007, and again in the same month in 2009, I was detained and interrogated by Canadian border officials on trips to British Columbia. The first time, they threatened to put me in a Canadian jail without charge, temporarily confiscated my passport and deported me. The second time, I was informed I had an FBI number. A criminal trial called the Olympia 22 that stemmed out of the 2006 port protests was also sabotaged by law enforcement... when they hacked into our attorney-client listserv."* (Dunn, 2014)

Writing for *The Seattle Globalist* in July 2014, Lael Henterly showed an example of the Domestic Terrorism Index developed by the JBLM Protection Division and how it was used to label political activists as domestic terrorists. The information entered into this Domestic Terrorism Index was fed to the WA State Fusion Center and to the Regional Intelligence Groups working with police departments throughout the state. (Henterly, 2014)

**DOMESTIC TERRORISM CONFERENCE
INDEX ENTRY FORM**

1. **DELETE** INDIVIDUAL/ORGANIZATION LISTED BELOW
WHICH APPEARS ON PAGE _____

2. **UPDATE** INDIVIDUAL/ORGANIZATION LISTED BELOW
WHICH APPEARS ON PAGE _____

3. **NEW** ENTRY LISTED BELOW X

NAME: Brendan M. Dunn DOB:

MONIKER/ALIASES: Maslauskas

ADDRESS: CITY: Olympia STATE/PROVINCE: WA

PHONE#: RACE: HEIGHT: WEIGHT:

SEX: EYE: HAIR:



The JBLM DES Protection Division is publishing daily reports about American citizens to INTELINK (<https://www.intelink.gov>), a United States Intelligence Community Database. Just what kind of information does an agency that is supposed to be maintaining the physical security of JBLM need to share with the United States Intelligence Community on a daily basis?



<https://inteldocs.intelink.gov/inteldocs/page/repository?path=%2FUser%2FFolders%2Fv%2Fve%2Fvessels%2FDaniel.L.vessels%2FJBLM%20Protection%20Daily>

Intelink is a group of secure intranets used by the United States Intelligence Community. Intelink-U (Intelink-SBU) is a sensitive but unclassified (SBU) variant of Intelink which was established for use by U.S. federal organizations and properly vetted state, tribal, and local officials so sensitive intelligence information could be shared amongst a secure community of interest.

Daniel L. Vessels is the Chief of the JBLM DES Protection Division, the agency accused in the lawsuit (Panagacos v. Towery) of violating the civil rights of hundreds of Americans by conducting an intensive, invasive, and illegal intelligence-gathering operation against people involved in political protest in Washington and Oregon.

The court case clearly showed that the JBLM DES Protection Division was (and obviously still is):

- illegally collecting and disseminating information about non-military-affiliated civilians
- illegally conducting electronic monitoring of social media accounts of non-military-affiliated civilians
- illegally entering email groups to gather information about political activities protected by the First Amendment
- illegally targeting political groups in Washington, listing their activities in intelligence databases and falsely describing their social and political activities as dangerous protests and a threat to the community.

Washington's Surveillance Complex

Washington State Fusion Center (WSFC) / Washington Joint Analytical Center (WAJAC)

WSFC is a federal, state, local and private sector partnership that encourages cross-agency information sharing. WSFC compiles information from a variety of sources (local law enforcement, Regional Intelligence Groups, Federal Agencies, and the Private Sector) and issues periodic Threat Assessments.

The WSFC replaced the WAJAC, which lacked guidelines for intelligence gathering and operated without accountability or oversight. (This was little more than a name change, the WSFC still operates without appropriate accountability or oversight.)

Regional Intelligence Groups

Regional Intelligence Groups (RIGs) are satellite offices that compile and distill information from local law enforcement. RIGs then feed information to WSFC.

Public files released by the Tacoma Police Department show that analysts do not limit their searches to groups associated with criminal behavior. Fusion center reports from Texas, Virginia and Missouri mirror this pattern.

Private Contractors

The Washington State Fusion Center is partially funded by a federal grant from the Department of Homeland Security. A clause in the grant requires that fusion center analysts paid with federal dollars be private, independent contractors. As noted in the Washington Statewide Integrated Intelligence Plan, Washington is also engaged in a broad effort to attract private sector participation in the fusion center. Experiences with private contractors taking over other government functions – including prisons and detention centers – causes us great concern. Such programs lack transparency and accountability.

The ACLU is actively litigated two cases with heavy overtones of government surveillance without suspicion. In *McCarthy v. Barrett*, The ACLU challenged unwarranted surveillance of individuals' First Amendment free speech activities as well as unjustified restrictions on lawful demonstrations. In *Chinn v. Blankenship**, the ACLU challenged the pre-textual stop and arrest of a young man on his way to an anti-war protest who was pulled over after his car was identified as carrying "three identified anarchists." (ACLU, 2010)

* It should be noted that Phillip Chinn was one of several individuals subjected to unlawful surveillance and harassment based on information provided to WA State law enforcement by the JBLM (Fort Lewis) DES Protection Division.



Information about you may also be entered into a system called eGuardian. The information entered into eGuardian is migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for further investigative action.

A significant problem with the eGuardian system is that the information entered into the system often lacks probable cause, or even a reasonable suspicion of criminal activity. Agencies with access to eGuardian can enter false or misleading information into the system, creating government records on American citizens who have done nothing wrong.

This was just what happened in 2020, 2022, and 2024 when anti-terrorism officers at the Joint Base Lewis-McChord (JBLM) DES Protection Division entered false information into the eGuardian system in order to harass and intimidate individuals who had

publicly objected to JBLM's monitoring and surveillance of civilian communities in violation of DOD regulations and Federal law.

Individuals whose names were entered into eGuardian would then be contacted by JTTF agents in an effort to intimidate them into silence and conceal the illegal surveillance and monitoring of civilian communities, throughout Washington, Oregon, and California, by the JBLM Anti-Terrorism Office (JBLMATO), JBLM DES Protection Division.

Requests for copies of the information entered into the eGuardian system are routinely denied, leaving individuals listed as a threat by some government agency with no way to review the allegations made against them or to challenge false and inaccurate information entered into the system.

The Brennan Center for Justice and New York University School of Law has said that the *“FBI Joint Terrorism Task Forces (JTTFs) inflict harm on local communities through racial profiling, harassment, suspicionless surveillance and investigations, and exploitation of immigration enforcement, all of which are authorized under federal guidelines loosened after 9/11. The FBI relies on the labor of state and local law enforcement officers assigned to the JTTFs, who agree to follow federal guidelines even if they conflict with state and local law, policies, and regulations. Civil rights advocates and community groups in*

Portland, San Francisco, and Oakland organized successful campaigns and lobbying operations to demand that their city legislatures hold local police accountable to local laws and ultimately withdraw from the JTTFs when the FBI refused to allow such public accountability. Advocates from each of these cities will discuss their efforts to organize public resistance to JTTF activities, enlist their elected representatives, craft legislation, and ultimately end local police participation in JTTFs, providing a model for other localities.” (Brennan Center, 2021)

While civil rights advocates in a few cities have been successful in getting local police departments to withdraw from the JTTF, there are many other departments that are still illegally gathering information about you and entering it into the eGuardian (and similar) databases.

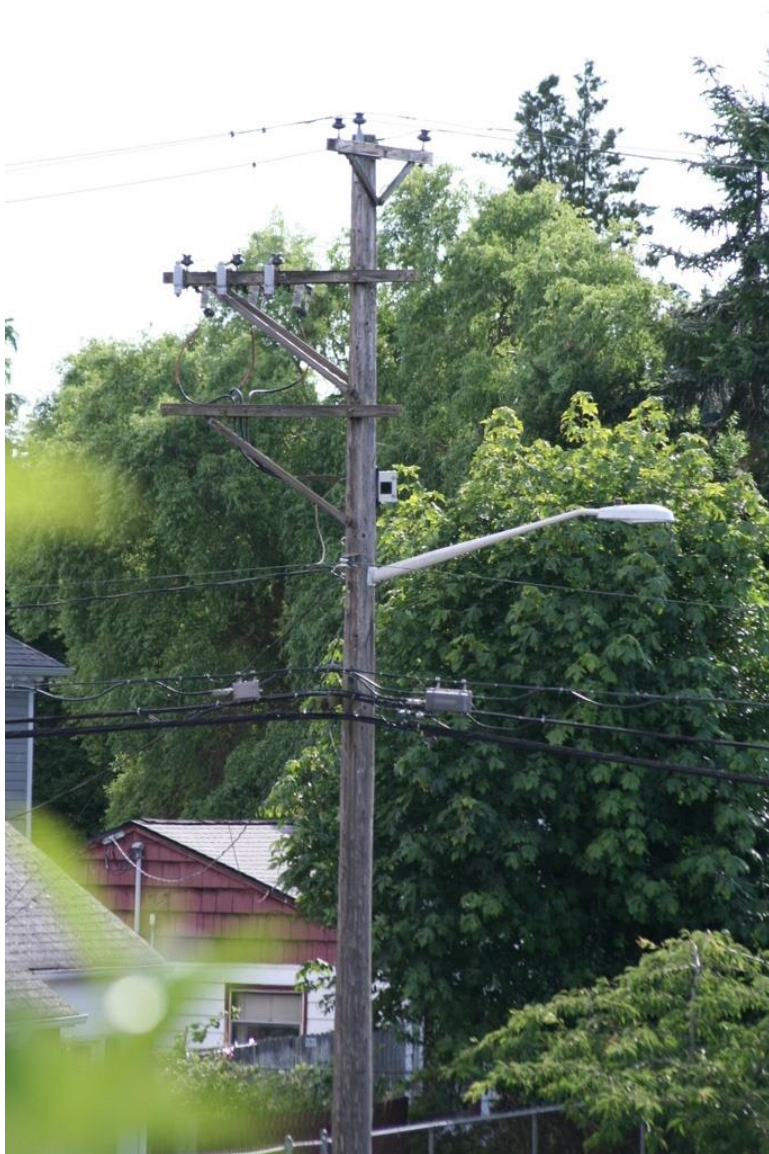
Cascade PBS reported in July 2023 that **"Pandemic relief funds are bankrolling new – and often unregulated – law enforcement tools such as license-plate readers, drones and AI video software."**

Across the state, one-time federal relief dollars are bankrolling increasingly sophisticated means of surveilling the public with few legal safeguards. Local governments have acquired mobile camera trailers, license-plate readers, gunshot detection software, drones and body cameras, and have installed security

cameras in parks, marinas, jails and courthouses. The expanded digital dragnet has the potential to feed into advanced AI-powered tools like facial recognition – which research has shown can reproduce the biases of its operators, potentially amplifying existing discriminatory policing practices against communities of color.

A recent report from the University of Washington’s Center for Human Rights warned that the vast quantity of data gathered and shared by license-plate reader cameras could aid attempts to deport migrants or prosecute out-of-state residents seeking abortions in Washington – two things state legislators have passed laws to discourage. The report cited Yakima, as well as police departments in Vancouver and Okanogan County, for feeding plate scans into commercial databases accessible to federal immigration enforcement agents and sharing plate data with police departments in states where abortion is a crime. (Block, 2023)

The following photos show a surveillance camera mounted on a utility pole outside of a home (Pitch Pipe) in Tacoma, WA.





(Concerned Independent Journalists, 2008)

While casual observations of a person's forays in and out of their home do not usually fall within the Fourth Amendment's protections, the US Supreme Court has held that this type of video surveillance of a person's home does violate the Fourth Amendment. The Court found that *"A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'"* [...] What's more, the Supreme Court recognized that long-term tracking of a person's movements *"provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"* (Cushing, 2019)



In the summer of 2020, there were large protests in both Portland and Seattle in response to the death of George Floyd at the hands of police. JBLM was present in both cities, using Stingray (JBLM records call these devices "Hailstorm") to

gather cell-phone data from everyone in the protest areas. The military enters the data they collect into INTELINK, JARVISS, and eGuardian databases and shares that information with their partners in the Washington State Fusion Center, the Oregon Titan Fusion Center, and various local police agencies. (Everbridge, 2023)

KGW8 News found Portland police spent more than 65 hours flying surveillance over protesters. The Center Square Oregon reported that the ACLU is suing Portland cops for 'unlawful' surveillance of protests. And The Intercept reported that an Air Force surveillance plane designed to carry state-of-the-art sensors typically reserved for war zones has been circling above Portland. (Iboshi, 2020) (Gruver, 2020) (Biddle, 2020)

Government surveillance is not just about gathering evidence of criminal activity. Surveillance is also a form of harassment and intimidation used against individuals in a malicious attempt to reduce the quality of their life so they will: be intimidated into silence, have a nervous break-down, become institutionalized, experience constant mental, emotional, or physical pain, become homeless, or even commit suicide.

In June 2023, it was reported that JBLM was denying veterans, military retirees and family members, access to medical care on the military installation and refusing them crisis counseling and access to suicide prevention resources, based on lists

developed by the JBLM DES Protection Division identifying veterans in crisis as posing a threat to good order and discipline on the military installation.

But this is nothing new at JBLM. **Madigan Army Medical Center employees, who have direct contact with hundreds of JBLM soldiers who have mental health diagnoses, stated that there is a pattern of soldiers with proven medical dysfunctions being kicked to the curb and dehumanized.** (Mirfendereski, 2019)

In August 2023, the San Francisco Bay Area Independent Media Center (Indybay) reported that "Joint Base Lewis-McChord, WA is "monitoring" addiction recovery meetings (AA / NA) (both on base and in the surrounding civilian communities) and keeping a database of individuals seeking recovery support, calling these people a "threat to good order and discipline". **No person can feel safe seeking addiction recovery support knowing that the JBLM ATO is infiltrating these recovery support meetings, recording vehicle license plates in the parking lots outside of places where these meetings are held, monitoring our cell-phone conversations, and keeping a database of Service Members, Family Members, Veterans, and Civilians in recovery** - claiming that these people pose a threat to good order and discipline on JBLM." (W., 2023)

In November 2023, further evidence of violence and corruption in the JBLM DES was

confirmed when video was leaked to the press that showed a JBLM civilian police officer (DACP) physically assaulting a female Soldier while she was in custody at the JBLM police station. According to the multiple news reports, senior police leadership on JBLM did not care about the assault on the Soldier. The individuals who provided this video to the news media also stated that they feared retaliation from the JBLM DES leadership for exposing this crime. A copy of the video is posted to the Q13 Fox (Seattle) YouTube channel. (Q13 Fox News (Seattle), 2023)

Public comments posted about this video and elsewhere on social media show a pattern of corruption, abuse, misconduct, and retaliation by the JBLM Police civilian leadership.



@paulhrabina161

I was a police officer there for many years. They managed to replace a lot of their older, more experienced officers with people totally unsuitable. Scholl was hired solely on the basis on being a friend of a manager, who was subsequently fired for claiming overtime he never worked, the JBLM management swept that under the rug rather do a criminal referral. The former Chief of Police who got promoted to Deputy Director of Emergency Services, only inhibition was he didn't want to go to jail, unethical yes, jail no, according to a conversation he had with one of the administrators. A deputy chief actually bragged about seeing to it I never worked as a police officer, before I had done anything wrong, personal grudge there.

One, they need to fix the audio.

Two, they will go completely nuts to find the guys that released this and retaliate. They will most definitely retaliate, they will do so on mere suspicion. The retaliation will consist of them doing major write ups on people who make even the slightest mistakes, misspellings, or even slight administrative mistakes that can easily be fixed with an eraser. The workplace environment is completely toxic. They also know that their jobs are secure, they'll ignore it, and it will blow over.

I am absolutely certain that if a review of their 15-6 investigations, which are low level investigations, is conducted by third parties, they will find evidence of criminal behavior which has been covered up and swept under the rug. The problem with sweeping things under the rug is that the bulges in the rug become noticeable.



Curt Casper Crappy civilian leadership has turned JBLM's civilian police into a joke. To be honest, if the army got rid of the civilians and replaced them with MP's law enforcement on the base may actually improve. It wasn't always the case.

Like · Reply

The Military Says You're a Terrorist if You Protest or Question the Government



According to a report by the San Francisco Bay Area Independent Media Center (Indybay) - An anti-terrorism brief was held on Fort Liberty (Fort Bragg) on July 10, 2024 where they listed several Pro-Life groups as "terrorist organizations." The Joint Base Lewis-McChord (JBLM), WA Anti-Terrorism Officer re-distributed this briefing, and when asked confirmed that JBLM identifies Pro-Life groups as "terrorist organizations" and individuals who express a Pro-Life ideology as "homegrown violent extremists". Following online controversy an official statement by the 18th Airborne Corps posted on the Fort Liberty Facebook page has disavowed the training product and the ideology contained on the slides, however, as these slides came from the unit responsible for installation access and security it is not clear if gate

guards were using this guidance to conduct unlawful ideologically motivated searches, flag certain license plates in their databases, or otherwise commit other Constitutional violations at Fort Liberty and Joint Base Lewis-McChord.

Regardless of whether you are Pro-Choice or Pro-Life, no matter how controversial your opinion or belief, the military has no right to label you a Terrorist for engaging in peaceful protests - but that is exactly what they are doing. (Indybay, The Military Say You're A Terrorist if You Protest or Question the Government, 2024)

In January 2024, news media reported that Pro-Palestinian protestors calling for a cease-fire and an end to the genocide in Gaza face an on-going threat of surveillance, monitoring, and harassment from the JBLM DES Protection Division. On Saturday, January 6th, 2024, Pro-Palestinian protestors calling for a cease-fire and an end to the genocide in Gaza blocked traffic on northbound I-5 between I-90 and SR-520, in Washington State. On Monday, January 8th, 2024, the Chief of the Joint Base Lewis-McChord (JBLM), Directorate of Emergency Services (DES) Protection Division briefed that the protestors opposing US support of Israel and the genocide in Gaza are homegrown violent extremists and pose a "domestic terrorist threat". JBLM stated that the military Protection Division would work with its "law enforcement partners" to identify and monitor pro-Palestinian protestors in Washington, Oregon, and California, and that more information about this threat would be included in his daily anti-terrorism protection

bulletin. Protester identification and information about their "activities, families, and associates" will be entered into the JARVISS database, as well as being reported in eGuardian for follow-up by the FBI's JTTF. (Indybay, JBLM Calls Pro-Palestinian Protestors in Seattle "Homegrown Violent Extremists", 2024)



Trust of Government

According to the Pew Research Center only about 2 in 10 (21%) of Americans believe that they can trust the government to do what is right “just about always” (2%) or “most of the time” (19%). (Pew Research Center, 2022)

When it comes specifically to trusting the police, Pew Research found that most Americans have at least some confidence in the police, but only 26% of Americans reported having “a great deal of confidence” in the police. The majority of those who reported having trust and confidence in the police were white, middle-aged, Americans who likely have little if any contact with the police on a regular basis. Minority populations reported far less confidence in the police, with up to two-thirds of Black men reporting that they had been unfairly stopped by the police, at least once. (Pew Research Center, 2022) What should be noted here is that three-quarters (74%) of Americans do NOT have a great deal of confidence in the police.

It should go without saying that speaking out against police violence or government overreach shouldn't land you in a surveillance database. But it can, and it does. According to the ACLU, they have received thousands of pages of public records revealing that law enforcement agencies are secretly acquiring social media spying software that can sweep activists [and other American citizens] into a web of digital surveillance. (Ozer, 2016)

It is clear that you cannot trust the police to tell the truth or to write accurate and unbiased reports. Furthermore, government agencies can use their police powers to target and harass anyone. As a police commander at Joint Base Lewis-McChord (JBLM) once said ***“You don’t have to actually have done anything wrong, we just have to make it look like you did.”*** Even if the police don’t win their case in court, they can and do use bogus citations as a means of harassment and retaliation.

Because we do not (cannot) trust the government and its armed enforcers – the police – it is important to develop a security culture as part of our normal lifestyle.

What Is Security Culture?

Security culture is a set of practices used to avoid, or mitigate the effects of, police surveillance and harassment and state control.

One of the best definitions of security culture was provided by Crimethinc in 2004, and begins: *“A security culture is a set of customs shared by a community whose members may be targeted by the government, designed to minimize risk. Having a security culture in place saves everyone the trouble of having to work out safety measures over and over from scratch, and can help offset paranoia and panic in stressful situations—hell, it might keep you out of prison, too. The difference between protocol and culture is that culture becomes unconscious,*

instinctive, and thus effortless; once the safest possible behavior has become habitual for everyone in the circles in which you travel, you can spend less time and energy emphasizing the need for it, or suffering the consequences of not having it, or worrying about how much danger you're in, as you'll know you're already doing everything you can to be careful. If you're in the habit of not giving away anything sensitive about yourself, you can collaborate with strangers without having to agonize about whether or not they are informers; if everyone knows what not to talk about over the telephone, your enemies can tap the line all they want and it won't get them anywhere."

The Ruckus Society says "A security culture is a set of customs and measures shared by a community whose members may engage in sensitive or illegal activities. Security culture practices minimize the risks of members getting arrested or their actions being foiled"

The Civil Liberties Defense Center (CLDC) stated: "Good security culture is one of the first and most important things a serious activist should learn. The idea is to minimize the effects of infiltration, disruption, and surveillance through practices that help keep activists, groups, and networks safer. Importantly, it helps political activists prevent paranoia and dispels the unfortunate idea that they should just give up any effort to maintain confidentiality against State and corporate surveillance."

The Deep Green Resistance News Service wrote: *“The modern surveillance state is unparalleled. Many people are legitimately afraid of state repression. But this fear can easily become paranoia and paralysis. As a result, some people will not get involved in radical organizing at all. Others will stay involved, but their paranoia will drive people away. The result? Our movements die. How do we combat this? By creating a “security culture” in our groups. Security culture is a set of practices and attitudes designed to increase the safety of political communities. These guidelines are created based on recent and historic state repression, and help to reduce paranoia and increase effectiveness.”*

A Practical Security Handbook for Activists and Campaigns (v 2.7) states: *“Security culture is important because we live in a world where upsetting the status quo to change the world for the better is generally met by a backlash. Governments, law enforcement agencies and corporations all have vested interests in criminalizing, disrupting and suppressing activist groups of all persuasions. Security culture is needed to ensure our continued success. We also have a basic right to protect our privacy and anonymity from unwarranted intrusion... Security culture is not a single thing; it is a process and a state of mind. You cannot put down and pick up security culture at whim. For security culture to be effective and worth the time and effort put into it, it has to be built into your life. Ideally, it becomes second nature; that is, you automatically go through*

the processes that keep you secure. This creates a mindset that helps you avoid errors of judgement you may regret later."

RATS, by: Claire Wolfe says *"These days, law enforcement at all levels -- from the local cop shop to obscure federal agencies -- uses snitches to trap ordinary people. Snitches tell lies that send their friends to jail. Paid agents provocateurs talk or trick otherwise harmless people into committing crimes. In many places, Snitch culture has virtually replaced real investigation of real crimes. Don't think you're exempt if you're a "law-abiding citizen." The most trusting, naive, innocent people often make the easiest targets for these weaselly, lying, opportunistic vermin. Snitches specialize in targeting the vulnerable."*

Basic Rules

There are "basic rules" that can help you protect yourself from government surveillance, harassment, and retaliation.

1) **Hide in the network.** Implement hidden services. Use Tor, I2P, Freenet, and VPNs to anonymize yourself. The less obvious you are, the safer you are. Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember, when in Rome, do as Romans do. Don't try to be a smart ass. Feds are many, Anonymous is Legion, but you are only one.

2) **Encrypt your communications.** Use TLS. Use IPsec. While it's true that some agencies target

encrypted connections - and may have explicit exploits against these protocols - you're much better protected than if you communicate in the clear. Woe betide anyone who transmits plaintext. Use as many security layers as possible. The question is not whether you are paranoid, but whether you are paranoid enough?

3) Assume that while your computer can be compromised, it would take work and risk to do so - so it probably isn't. Still physical security is important and should be included in your overall personal security plan.

4) Be suspicious of commercial encryption software, especially from large vendors. It is likely that most encryption products from large US companies have back doors, and many foreign ones probably do as well. It's prudent to assume that foreign products also have foreign-installed backdoors. Closed-source software is easier to backdoor than open-source software. Systems relying on master secrets are vulnerable to adversaries, through either legal or more clandestine means.

5) Use public-domain encryption that has to be compatible with other implementations. For example, it's harder to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving an adversary a lot more freedom to make changes. And because BitLocker is proprietary, it's far less likely those

changes will be discovered. Prefer symmetric cryptography over public-key cryptography. Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that governments influence when they can.

6) Security is a continuing process, not a state.

Never become complacent! Do security audits on a regular basis. And do encrypted backups. Backups are important, as there are two types of people, those who have backups and those who have lost their data.

7) Always browse in "Private Mode" so that fewer traces of your web history remain on your HDD.

Opera, Chrome, Firefox, Safari, and Internet Explorer all include a form of Private Browsing. Regularly clean your computer using programs such as BleachBit or CCleaner.

8) Do NOT tell anyone anything that could get you in trouble.

Assume anything can get you in trouble, because it probably will, especially with any government official. Remember anyone looking to gain a favor with the state can and will snitch on you.

Don't Talk to the Police - Ever! "Any lawyer worth his salt will tell the suspect in no uncertain terms to make no statement to police under any circumstances." (U.S. Supreme Court Justice Robert H. Jackson writing in *Watts v. Indiana*, 338 U.S. 49 (1949))

9) Do NOT keep anything that can be used as evidence against you. Even the most truthful and innocent statement can be used to bring criminal charges against you. “The complexity of modern federal criminal law, codified in several thousand sections of the United States Code and the virtually infinite variety of factual circumstances that might trigger an investigation into a possible violation of the law, make it difficult for anyone to know, in advance, just when a particular set of statements might later appear (to a prosecutor) to be relevant to some such investigation.” (U.S. Supreme Court Justice Stephen Breyer, writing in *Rubin v. United States* 524 U.S. 1301 (1998))

10) Know where the cameras are and how to avoid them. Know who patrols where, and what routine they follow so as to avoid contact. Find ways around checkpoints; use side streets, forest paths, neighbors' yards, railroad tracks, tunnels; whatever route is necessary to getting from point A to point B without a pack of government agents searching you, checking your ID, or having your image recorded by Big Brother.

11) Do the unexpected. Do not settle into a routine that invites easy attack or allows anticipation of your aims and activities.

12) Don't talk to strangers! Beware of Infiltrators, Informers and Grasses. The more you post on-line, the easier you are to target.

13) Mistrust authority — promote decentralization.

The majority of people in developed countries spend at least some time interacting with the Internet, and hostile Governments are abusing that necessity in secret to extend their powers beyond what is necessary and appropriate. Even if you're not doing anything wrong, you're being watched and recorded... it has reached the point where you don't have to have done anything wrong, you simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life.

14) Never leave things lying about unattended or lay them down where you are liable to forget them.

Learn to write lightly; the "blank" page underneath has often been read. If you have to destroy a document, do so thoroughly. Carry as little written matter as possible, and for the shortest possible time. Never carry names or addresses en clair. If you cannot carry them for the time being in your head, put them in a species of personal code, which only you understand.

15) Make as many of your difficult appointments as you can after dark.

Turn the night to good use. If you cannot make it after dark, make it very early morning when people are only half awake and not on the lookout for strange goings-on.

Rules of Clandestine Operations

By Jellam forney @ 2001
www.jellamforney.com

MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER. BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

Be careful. Be cool.

...and keep your fucking mouth shut!

JEFF STEINBORN
FOR 33 YEARS, SEATTLE LAWYER HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, **MARIJUANA: THE LAW, & YOU** IS ON HIS WEBSITE: www.potbust.com (LOTS A LINES TOO!)

HERE'S JEFF'S ADVICE---

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME:
(the safest place to smoke)

1 Smoke out back.
KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REeks OF POT.

2 Be tidy.
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.
Hello, sir! A lost cat-- HEY!
Shift!
NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

3 The phone.
NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.
Can I come over?
YES!
I'd like 2 green sweaters, and a mushroom pizza.
NO!

4 Email.
KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.
Consider any email PUBLIC.

IN PUBLIC:

5 Smoke joints.
ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE. SMOKE IT LIKE A CIGARETTE. PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR YOUR POCKET) SHE'LL FIND A HARD OBJECT & CAN PULL IT OUT.
Sloppy joint-rolling machines are cheap.

IN YOUR CAR:

6 Be a moving target.
PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINTS, AND THEN STASH IT.
YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

7 Again--be tidy.
KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.
hollowed-out Sharpie
BAGGIES IN THE GLOVEBOX WHEN YOU GO FOR YOUR REGISTRATION? JOINT IN YOUR WALLET WHEN YOU'RE PULLING OUT YOUR ID? Tsk!!

8 One law at a time.
IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE, & WEAR YOUR SEAT BELT.
AND DON'T HAVE ANY OUTSTANDING WARRANTS!

IN GENERAL:

9 Camouflage is good.
DON'T LOOK LIKE A POTHEAD.
A SQUARE IS LESS OF A TARGET THAN A FREAK.
SAY AND UNFAIR, BUT TRUE.

A compilation of the "Rules of Secret Work", from the SACP (via KGB?), "The Ten Crack Commandments" by Biggie Smalls, unwritten rules of the professional thief, the CIA's Moscow rules, rules

for how to smoke pot and not go to jail, and my own 10 OPSEC commandments.

The Rules:

1. Always have a believable' legend to cover your work!

- Live your legend
- Vary your pattern, and stay within your cover

2. Underground membership must be secret!

- Never reveal your operational details
- Never reveal your plans
- Seven: this rule is so underrated / Keep your family and business completely separated
- Compartment sensitive information and keep it secret

3. Behave naturally and do not draw attention to yourself! `Be like the people'. Merge with them!

- Go with the flow. Blend in
- Maintain a natural pace
- Lull them into a sense of complacency
- Camouflage is good

4. No loose talk! Guard secrets with your life! Follow the saying: `Don't trust anyone and talk as little as possible'.

- Need to know - follow it
- STFU

- Rule nombre uno: never let no one know / How much, dough you hold
- Number two: never let em know your next move / Don't you know Bad Boys move in silence or violence
- Be proactively paranoid, it doesn't work retroactively

5. Be vigilant against informers! They try to get close to you, using militant talk to 'test' and trap you.

- Number three: never trust no-bo-dy
- Everyone is potentially under opposition control.

6. Be disciplined, efficient, punctual. Only wait ten minutes at a meeting place. The late comer may have been arrested.

- Professional thieves are punctual to meetings, a late arrival indicates arrest

7. Make all preparations beforehand! Avoid a regular pattern of behavior which makes it easy for the enemy to check on you.

- Build in opportunity, but use it sparingly
- Vary your pattern and stay within your cover
- Pick the time and place for action
- Keep your options open

8. Do not try to discover what does not concern you! Know only what you have to know for carrying out your tasks.

- Need to know - if you don't need to know it, it is better that you don't

9. Be careful what you say on the phone (which may be 'bugged'), or in a public place! Conceal sensitive information such as names etc. by using simple codes!

- Always use cryptonyms and "open codes" to discuss sensitive topics
- Avoid keywords

10. Remove all traces of illegal work that can lead to you! Wipe fingerprints off objects. Know that communiques can be traced; goods bought from shops can be checked.

- Maintain cautious habits
- Be tidy, clean up after yourself. Don't leave illicit goods or data around for anyone to find

11. Hide materials such as leaflets, weapons etc.! But not where you live. Memorize sensitive names, addresses etc. Don't write them down!

- Number five: never sell no crack where you rest at / I don't care if they want an ounce, tell em to bounce
- Number eight: never keep no weight on you
- Professional thieves stash illicit goods at restaurants, drug stores, cigar shops, etc.

12. Carry reliable documents of identification!

13. Know your town, its streets, parks, shops etc. like the palm of your hand! This will help you find secret

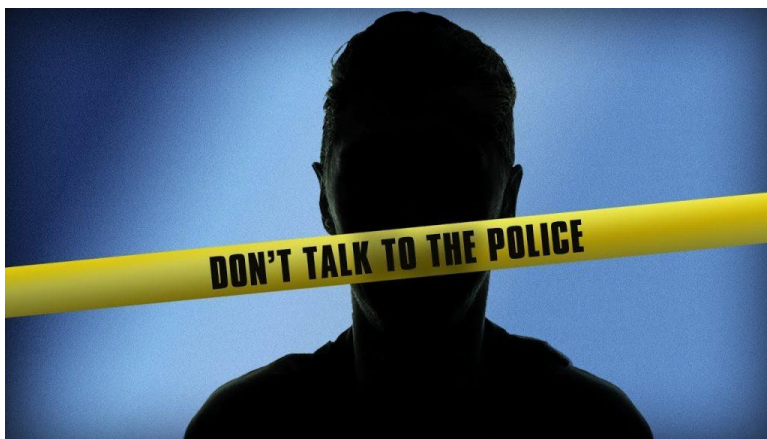
places and enable you to check whether you are being followed.

- Own the street

14. If you are arrested you must deny all secret work and never reveal the names of your comrades even to the point of death!

15. Finally, if any member of your underground cell is arrested, you must immediately act on the assumption that they will be forced to give information. This means taking precautions, such as going into hiding if necessary.

When the rules of secrecy are practiced revolutionaries make good progress. Practice makes perfect and with discipline and vigilance we will outwit the enemy and we will win! Amateurs practice until they get it right, professionals practice until they can't get it wrong.



Resources

The following resources can help you develop a security culture and protect yourself against government surveillance, spying, and harassment:

ACLU of Washington - Know Your Rights

(<https://www.aclu-wa.org/know-your-rights>)

Autistici/Inventati (<https://www.autistici.org/>)

Civil Liberties Defense Center (<https://cldc.org/>)

Disroot (<https://disroot.org/en>)

Electronic Frontier Foundation - Surveillance Self-Defense (<https://ssd.eff.org/>)

National Lawyers Guild - Know Your Rights

(<https://www.nlg.org/know-your-rights/>)

Privacy Tools (<https://www.privacytools.io/>)

RATS! Your guide to protecting yourself against snitches, informers ... (<https://rats-nosnitch.com/>)

Restore Privacy (<https://restoreprivacy.com/>)

Riseup (<https://riseup.net/>)

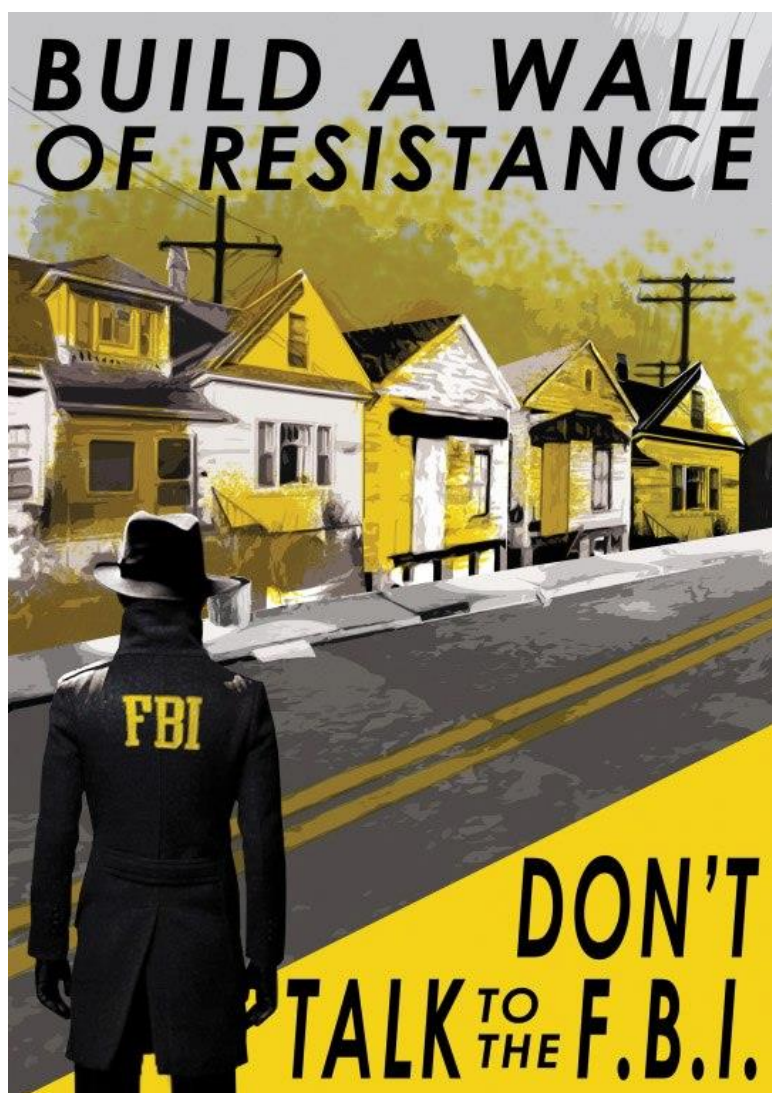
Security-in-a-Box - Front Line Defenders

(<https://securityinabox.org/en/>)

The Gurgq – Underground Trade Tradecraft

(<https://grugq.tumblr.com/post/60463307186/rules-of-clandestine-operation>)

Tuta (<https://tuta.com/>)

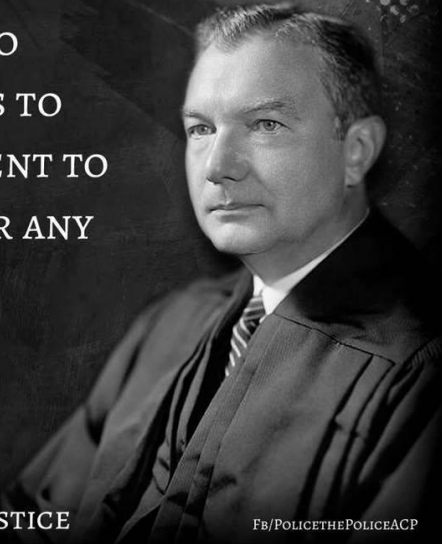


DON'T TALK TO POLICE

“ANY LAWYER WORTH
HIS SALT WILL TELL
THE SUSPECT IN NO
UNCERTAIN TERMS TO
MAKE NO STATEMENT TO
THE POLICE UNDER ANY
CIRCUMSTANCES.”

Robert Jackson

FORMER U.S.
ATTORNEY GENERAL
AND SUPREME COURT JUSTICE



FB/POLICE THE POLICE ACP

Remember...

- **I want a lawyer.**
- **I do not consent to a search.**
- **I am going to remain silent.**

Works Cited

- ACLU. (2010, June 28). *Government Agencies to Pay \$418,000 in Political Surveillance Case*. Retrieved from American Civil Liberties Union of Washington: <https://aclu-wa.org/news/government-agencies-pay-418000-political-surveillance-case>
- ACLU. (2022, June). *Privacy and Surveillance*. Retrieved from American Civil Liberties Union: <https://www.aclu.org/issues/national-security/privacy-and-surveillance>
- Biddle, S. (2020, July 23). *An Air Force Special Operations Surveillance Plane Is Lurking Near Portland During Federal Crackdown*. Retrieved from The Intercept: <https://theintercept.com/2020/07/23/air-force-surveillance-plane-portland-protests/>
- Block, B. (2023, July 26). *Federal Aid is Supercharging Local WA Police Surveillance Tech*. Retrieved from Cascade PBS: <https://crosscut.com/investigations/2023/07/federal-aid-supercharging-local-wa-police-surveillance-tech>
- Brennan Center. (2021, February 21). *Bad Partners: Why Local Law Enforcement Should Leave FBI Joint Terrorism Task Forces*. Retrieved from Brennan Center: <https://www.brennancenter.org/events/bad-partners-why-local-law-enforcement-should-leave-fbi-joint-terrorism-task-forces>
- Center for Constitutional Rights. (2022, July). *Government Surveillance*. Retrieved from Center for Constitutional Rights: <https://ccrjustice.org/home/what-we-do/issues/government-surveillance>
- Concerned Independent Journalists. (2008, July 10). *Tacoma: Pitch Pipe Infoshop Under Surveillance*. Retrieved from

San Francisco Bay Area Independent Media Center
(Indybay):
<https://www.indybay.org/newsitems/2008/07/10/18515172.php>

Cushing, T. (2019, June 10).
<https://www.techdirt.com/articles/20190609/10585442362/federal-court-eight-months-utility-pole-camera-surveillance-is-fourth-amendment-violation.shtml>.
Retrieved from TechDirt:
<https://www.techdirt.com/articles/20190609/10585442362/federal-court-eight-months-utility-pole-camera-surveillance-is-fourth-amendment-violation.shtml>

Defending Rights and Dissent. (2014, February 24). *New Docs Show Army Coordinated Spy Ring*. Retrieved from
Defending Rights and Dissent:
<https://www.rightsanddissent.org/news/new-docs-show-army-coordinated-spy-ring/>

Democracy Now. (2013, June 10). “*You’re Being Watched*”:
Edward Snowden Emerges as Source Behind Explosive Revelations of NSA Spying. Retrieved from Democracy
Now:
https://www.democracynow.org/2013/6/10/youre_being_watched_edward_snowden_emerges

Dunn, B. M. (2014, April). *New evidence shows U.S. government spied on Wobblies, activists*. Retrieved July 3, 2018,
from <https://libcom.org/library/new-evidence-shows-us-government-spied-wobblies-activists>

Esteban, M. (2018, November 8). *The spy in your pocket; How your phone can be tricked*. Retrieved from KOMO 4
News: <https://komonews.com/news/local/a-spy-in-your-pocket>

- Everbridge. (2023). *Joint Analytic Real-Time Virtual Information Sharing System (JARVISS)*. Retrieved from Everbridge: <https://www.everbridge.com/products/jarviss/>
- Fakhoury, H. (2015, 04 30). *Military Internet Surveillance of Civilians Must Be Excluded From Criminal Trials*. Retrieved from ACLU of Washington: <https://aclu-wa.org/blog/military-internet-surveillance-civilians-must-be-excluded-criminal-trials>
- Gruver, T. (2020, July 29). *ACLU sues Portland cops for 'unlawful' surveillance of protests*. Retrieved from The Center Square: https://www.thecentersquare.com/oregon/aclu-sues-portland-cops-for-unlawful-surveillance-of-protests/article_4087eb32-d215-11ea-b9a5-83aa3d3bb6d4.html
- Gurman, S. (2016, September 27). *AP: Across US, police officers abuse confidential databases*. Retrieved from AP News: <https://apnews.com/article/699236946e3140659fff8a2362e16f43>
- Henterly, L. (2014, July 25). How to Prove the Government is Spying on You. *The Seattle Globalist*, pp. <http://www.seattleglobalist.com/2014/07/25/how-to-prove-the-government-is-spying-on-you/27863>.
- Hermes, K. (2017, April 3). *Antiwar Activists Challenge Army's Domestic Spying Apparatus in Ninth Circuit*. Retrieved from Huffington Post: https://www.huffpost.com/entry/antiwar-activists-challenge-armys-domestic-spying_b_58e173e7e4b0ca889ba1a74e
- Iboshi, K. (2020, June 12). *Who is flying circles over Portland protests?* Retrieved from KGW8 News:

<https://www.kgw.com/article/news/investigations/who-is-flying-circles-over-portland-protests/283-1aab235b-092f-4430-ab17-632e8fb7c8a7>

Indybay. (2024, January 8). *JBLM Calls Pro-Palestinian Protestors in Seattle "Homegrown Violent Extremists"*. Retrieved from San Francisco Bay Area Independent Media Center (Indybay):

<https://www.indybay.org/newsitems/2024/01/08/18861680.php>

Indybay. (2024, July 11). *The Military Say You're A Terrorist if You Protest or Question the Government*. Retrieved from San Francisco Bay Area Independent Media Center:

<https://www.indybay.org/newsitems/2024/07/11/18867943.php>

JBLM Cop Watch. (2022, January 3). *JBLM DES Protection Division Still Illegally Spying On You*. Retrieved from San Francisco Bay Area Independent Media Center (Indybay) :

<https://www.indybay.org/newsitems/2022/01/03/18847078.php>

Lennard, N. (2023, November 8). *Oregon Police Obsessively Spied on Activists for Years...* Retrieved from The Intercept:

<https://theintercept.com/2023/11/08/oregon-police-surveillance-protests-activists/>

Levering, L. M. (2011, August 4). *There's no such thing as too vigilant, official say*. Retrieved from Northwest Guardian:

http://www.nwguardian.com/2011/08/04/10767_there-s-no-such-thing-as-too-vigilant.html

- Martin, K. (2016, February 25). *Tacoma police using surveillance device to sweep up cellphone data*. Retrieved from Tacoma News Tribune:
<https://www.thenewstribune.com/news/local/article25878184.html>
- Mirfendereski, T. (2019, August 7). *Whistleblowers: Army ignoring advice of medical experts*. Retrieved from KING5 News:
<https://www.king5.com/article/news/local/investigations/whistleblowers-army-punishes-jblm-soldiers-who-need-help/281-616155891>
- Ozer, N. (2016, September 22). *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*. Retrieved from ACLU:
<https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software>
- Pawloski, J. (2011, January 25). *Ex-worker at JBLM collected activist data*. Retrieved from Olympian Newspaper:
<https://www.theolympian.com/news/local/article25280662.html>
- Pew Research Center. (2022, June 6). *Public Trust in Government: 1958-2022*. Retrieved from Pew Research:
<https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/>
- Pew Research Center. (2022, January 5). *Trust in America: Do Americans trust the police?* Retrieved from Pew Research:
<https://www.pewresearch.org/2022/01/05/trust-in-america-do-americans-trust-the-police/>

Q13 Fox News (Seattle). (2023, November 15). *Whistleblowers Call JBLM's Police System Broken*. Retrieved from <https://www.youtube.com/watch?v=ejw0no3imuY>

Q13 Fox News. (2021, August 5). *Docs: FBI arrests Washington man charged in Capitol riot after mom posts his pic on Facebook*. Retrieved from Q13 Fox News: <https://www.q13fox.com/news/docs-fbi-arrests-washington-man-charged-in-capitol-riot-after-mom-posts-his-pic-on-facebook>

W., B. (2023, August 30). *The Military is Spying on AA Meetings*. Retrieved from San Francisco Bay Area Independent Media Center (Indybay): <https://www.indybay.org/newsitems/2023/08/30/18858608.php>